Abelian varieties over number fields, tame ramification and big Galois image

Sara Arias-de-Reyna Christian Kappen

Abstract

Given a natural number $n \geq 1$ and a number field K, we show the existence of an integer ℓ_0 such that for any prime number $\ell \geq \ell_0$, there exists a finite extension F/K, unramified in all places above ℓ, together with a principally polarized abelian variety A of dimension n over F such that the resulting ℓ-torsion representation

$$\rho_{A,\ell} : G_F \to \mathrm{GSp}(A[\ell](\overline{F}))$$

is surjective and everywhere tamely ramified. In particular, we realize $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ as the Galois group of a finite tame extension of number fields F'/F such that F is unramified above ℓ.

1 Introduction

Let ℓ be a prime number. In this paper, we establish results regarding the existence of abelian varieties A over number fields F such that the representation $\rho_{A,\ell}$ of the absolute Galois group G_F of F on the symplectic $\mathbb{F}_\ell$-vector space of geometric ℓ-torsion points of A satisfies certain local and global conditions. More specifically, we are interested in finding A/F such that $\rho_{A,\ell}$ is everywhere tamely ramified and has large image.

Our interest in such objects A/F was inspired by the tame inverse Galois problem over the rational field $\mathbb{Q}$: if one could construct $A/\mathbb{Q}$ of dimension $n \geq 1$ such that

(i) $\rho_{A,\ell}$ is everywhere tamely ramified and

(ii) $\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ is surjective,

then the finite Galois extension $(\overline{\mathbb{Q}})^{\ker \rho_{A,\ell}}/\mathbb{Q}$ would be tamely ramified with Galois group $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$, thus providing a solution to the tame inverse Galois problem over $\mathbb{Q}$ for the group $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. Let us note that tameness is only a condition at the primes p dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. Let us further note that if p is a prime different from ℓ such that A has good reduction at p, then $\rho_{A,\ell}$ is unramified (and hence tame) at p, by the criterion of Néron-Ogg-Shafarevich.

In previous work, the first author has constructed, for each prime number ℓ, infinitely many nonisomorphic non-CM elliptic curves over $\mathbb{Q}$ having good supersingular reduction at ℓ (see

[3]); these elliptic curves satisfy the two conditions listed above. For abelian varieties of arbitrary dimension with good supersingular reduction at ℓ, she has isolated a condition, called Hypothesis (H), which is sufficient to imply tame ramification at ℓ (see [1]). Hypothesis (H) is a condition on the valuations of the coordinates of the ℓ-torsion points of the group attached to the formal group law of the abelian variety. Using very explicit equations she manages to obtain, for each ℓ, infinitely many abelian surfaces over $\mathbb{Q}$ arising as Jacobians of suitable curves, satisfying Hypothesis (H) and having trivial absolute endomorphism ring (see [4]). Her construction proceeds roughly as follows: she first finds a suitable genus two curve locally at ℓ which, in a second step, is globalised; the resulting curve over $\mathbb{Q}$ is then deformed in order to also satisfy requirements at primes different from ℓ, requirements which ensure certain global properties (e.g. large image of the resulting Galois representation).

This approach to the problem relies on very explicit computations on the Jacobians of genus two curves, methods which are not available in higher dimensions. To address the question whether there exist higher-dimensional abelian varieties with the property that the Galois representation on the ℓ-torsion points is tame and has large image, we follow a more conceptual approach: we consider a suitable moduli space of abelian varieties, and we prove the existence of a point P on this space defined over some number field unramified above ℓ such that P satisfies certain local conditions at a finite number of finite places, properties that will ensure tame ramification and large image. Our main result is the following:

Theorem 1.1. *Given a number field K and an integer $n \geq 1$, there exists an integer ℓ_0 such that, for all prime numbers $\ell \geq \ell_0$, there exist a finite extension F of K, unramified in all places above ℓ, and an n-dimensional abelian variety A defined over F such that the associated ℓ-torsion representation $\rho_{A,\ell} : G_F \to \mathrm{GSp}(A[\ell](\overline{F}))$ is surjective and everywhere tamely ramified.*

As a corollary, we obtain, for almost all prime numbers ℓ, the group $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ as the Galois group of a finite extension F'/F of number fields, where F is unramified above ℓ. Let us note, however, that this result is a special case of [7] Prop. 3.2, which solves the potential tame inverse Galois problem in full generality, i.e. for arbitrary finite groups, even with the imposition of local conditions at a finite number of primes. Our construction nevertheless provides a tamely ramified surjective Galois representation which comes from the ℓ-torsion of a suitable abelian variety defined over a number field and, hence, is a member of a compatible system of Galois representations.

Let us outline the structure of the present paper. In Section 2 we give, for $\ell \geq 3$, a criterion for the ℓ-torsion representation $\rho_{A,\ell}$ of an n-dimensional abelian variety defined over a number field K to be surjective onto $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$: we find that $\rho_{A,\ell}$ is surjective if the degree of the field extension $K(\mu_\ell)/K$ obtained by adjoining to K the ℓ-th roots of unity equals $\ell - 1$ and if furthermore the image of $\rho_{A,\ell}$ contains a transvection as well as an element whose characteristic polynomial is irreducible and has nonzero trace. (In the appendix, we show that such elements always exist in $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ if $\ell \geq 5$ and $\ell \nmid n$). In Section 3, we revisit some tools from arithmetic geometry which we will need in the proof of Theorem 1.1, namely Moret-Bailly's theorem on the existence of global points and Kisin's results on local constancy in p-adic families of Galois representations. In Section 4, we set up some notation, and we apply the tools from the previous section to develop a series of useful results about existence of abelian varieties with prescribed properties that will be combined in the proof of the main

result. In Section 5, we give the proof of Theorem 1.1, and we mention some open questions. Let us briefly outline the strategy of the proof of Theorem 1.1:

Using the appendix of this paper and results of Hall and Kowalski ([13]), we find, after possibly extending K, an integer $\ell_0 > j$ and a Jacobian J over K admitting a full symplectic level j structure (for some prefixed integer $j \geq 3$) such that $\mu_j \subseteq K$ and such that for all prime numbers $\ell \geq \ell_0$, $K/\mathbb{Q}$ is unramified at ℓ, and the image of the ℓ-torsion representation $\rho_{J,\ell}$ of J contains an irreducible element of nonzero trace $\mathfrak{s}$ and a transvection $\mathfrak{t}$. Let $K'' = K(J[\ell], J[j])$, and let S denote the set of finite places of K dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. We find finite extensions $(K'_\nu/K_\nu)_{\nu \in S}$ of common degree r together with elliptic curves of good reduction E_ν/K'_ν, defined over $\mathbb{Q}$, admitting full symplectic level j structures, where for $\nu|\ell$ the reduction of E_ν is in addition supersingular. We then find a finite extension K'/K of degree r that is linearly disjoint from K''/K and that induces the local extensions K'_ν/K_ν. After replacing K by K', the elliptic curves E_ν with their level structures are defined over the K_ν, and the elements $\mathfrak{s}$ and $\mathfrak{t}$ still lie in the image of $\rho_{J,\ell}$. By Čebotarev's density theorem, there exist finite places $\mu_\mathfrak{s}$ and $\mu_\mathfrak{t}$ of K away from S such that $\mathfrak{r} \in \{\mathfrak{s}, \mathfrak{t}\}$ is the $\rho_{J,\ell}$-image of a Frobenius element at $\mu_\mathfrak{r}$. We set $S' = S \cup \{\mu_\mathfrak{s}, \mu_\mathfrak{t}\}$. Let $\mathcal{A} = \mathcal{A}_{n,1,j/K}$ denote the K-variety parametrizing principally polarized n-dimensional abelian varieties with full level j structure. For each $\nu \in S$, let $x_\nu \in \mathcal{A}(K_\nu)$ denote the point defined by E_ν^n, and for $\mathfrak{r} \in \{\mathfrak{s}, \mathfrak{t}\}$, let $x_{\mu_\mathfrak{r}} \in \mathcal{A}(K_\nu)$ denote the point defined by $J \otimes_K K_{\mu_\mathfrak{r}}$. By Kisin's results on local constancy of families of Galois representations (cf. [14]), there exists, for each $\nu \in S'$, a ν-adically open neighborhood Ω_ν of x_ν such that for each $y_\nu \in \Omega_\nu$, the resulting representations $\rho_{x_\nu,\ell}$ and $\rho_{y_\nu,\ell}$ coincide up to conjugation by elements in $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. By a result of Moret-Bailly (cf. [17]), there exists a finite field extension F/K linearly disjoint to $K(\mu_\ell)/K$ together with a point $y \in \mathcal{A}(F)$ such that the places $\nu \in S'$ split completely in F and such that $y_\nu \in \Omega_\nu$ for all $\nu \in S'$. The abelian variety A/F defined by y has then the property that $\rho_{A,\ell}$ is tamely ramified in all places of F dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ and that the image of $\rho_{A,\ell}$ contains conjugates of $\mathfrak{s}$ and $\mathfrak{t}$. Now $\rho_{A,\ell}$ is everywhere tamely ramified, and $\rho_{A,\ell}$ maps onto $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. All the extensions of K that we made in the above proof can be chosen to be unramified in the places above ℓ, and F/K is totally split in the places above ℓ; hence F is unramified above ℓ, as desired.

Let us remark that if we dropped the requirement on F of being unramified above ℓ, there would be an easier way to find A/F: we could then simply consider the Jacobian J/K above and eliminate ramification in primes dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ by means of a finite extension F/K that is orthogonal to $K(J[\ell])$.

The first author worked on this project as a research fellow of the Alexander von Humboldt Foundation; she was partially supported by the Ministerio de Educación y Ciencia grant MTM2009-07024. The second author was partially supported by the SFB 45 "Periods, moduli spaces and arithmetic of algebraic varieties", and he would like to thank the University of Luxembourg for its hospitality. Both authors would like to thank Brian Conrad, Ulrich Görtz and Gabor Wiese for helpful discussions. They would also like to thank the anonymous referee, for his useful remarks and his very helpful suggestions regarding the overall structure of the paper.

2 Surjectivity of representations attached to abelian varieties

Let $\ell \geq 3$ be a prime number, let n be a positive integer, and let V be a $2n$-dimensional vector space over $\mathbb{F}_\ell$ endowed with a symplectic form. Let us recall the following result (cf. Theorem 2 of [15], Theorem 1.1 of [2]):

Theorem 2.1. *Let $G \subset \mathrm{GSp}(V)$ be a subgroup containing a transvection. Then exactly one of the following statements holds:*

(*i*) *The action of G on V is reducible in the sense that it stabilizes a nontrivial nonsingular symplectic subspace.*

(*ii*) *There exists a proper decomposition $V = \bigoplus_{i\in I} S_i$ of V into equidimensional nonsingular symplectic subspaces S_i such that for each $g \in G$ and each $i \in I$, there exists some $j \in I$ with $g(S_i) \subseteq S_j$ and such that the resulting action of G on I is transitive.*

(*iii*) $G \supset \mathrm{Sp}(V)$.

From this statement we can derive a useful criterion ensuring that a group $G \subset \mathrm{GSp}(V)$ contains $\mathrm{Sp}(V)$:

Corollary 2.2. *Let $G \subset \mathrm{GSp}(V)$ be a subgroup containing a transvection and an element of nonzero trace whose characteristic polynomial is irreducible. Then $G \supset \mathrm{Sp}(V)$.*

Proof. Since G contains a transvection, we are in one of the three cases of Theorem 2.1. Let $g \in G$ be an element of nonzero trace whose characteristic polynomial is irreducible. First of all, g acts irreducibly on V, and hence the action of G on V cannot be reducible, which excludes case (*i*). Assume now that we are in case (*ii*), i.e. that G preserves a nontrivial decomposition $V = \bigoplus_{i=1}^{h} S_i$. Since g acts irreducibly, it cannot fix any of the S_i; hence the trace of g must be zero, which leads to a contradiction. We conclude that only case (*iii*) of Theorem 2.1 is compatible with the existence of g. □

Remark 2.3. In the Appendix, we prove that if n is any positive integer and ℓ is an odd prime, then if $r \in \mathbb{N}$ is such that ℓ^r is sufficiently large, then the polynomial ring $\mathbb{F}_{\ell^r}[X]$ contains an irreducible symplectic polynomial of nonzero-trace and of degree $2n$.

If K is a number field, if $\overline{K}$ is an algebraic closure of K and if A is a principally polarized abelian K-variety of dimension n, we let $A[\ell](\overline{K})$ denote the $\mathbb{F}_\ell$-vector space of geometric ℓ-torsion points of A; it is a $2n$-dimensional vector space over $\mathbb{F}_\ell$, and the Weil pairing gives rise to a non-degenerate symplectic form $\langle\cdot,\cdot\rangle : A[\ell] \times A[\ell] \to \mu_\ell$, where μ_ℓ denotes the finite étale K-group scheme of ℓ-th roots of unity. By functoriality, the action of $G_K = \mathrm{Gal}(\overline{K}/K)$ on $A[\ell](\overline{K})$ and on $\mu_\ell(\overline{K})$ commutes with this pairing. That is, if we let χ_ℓ denote the mod ℓ cyclotomic character, then for all $\sigma \in G_K$ and for all $P_1, P_2 \in A[\ell](\overline{K})$,

$$\langle P_1^\sigma, P_2^\sigma\rangle = \chi_\ell(\sigma)\langle P_1, P_2\rangle \ ,$$

which compels the image of the representation $\rho_{A,\ell} : G_K \to \mathrm{Aut}(A[\ell](\overline{K}))$ to be contained in the general symplectic group $\mathrm{GSp}(A[\ell](\overline{K})) \simeq \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. If $[K(\mu_\ell) : K] = \ell - 1$, then χ_ℓ is

surjective. In this case, if the image of $\rho_{A,\ell}$ contains $\mathrm{Sp}(A[\ell](\overline{K}))$, it must already coincide with $\mathrm{GSp}(A[\ell](\overline{K}))$.

Since a number field contains only a finite number of roots of unity, this observation implies the following result:

Lemma 2.4. *Let K be a number field. Then there exists an integer ℓ_0 such that for all primes $\ell \geq \ell_0$ and all abelian varieties A/K, the following holds: if the image of $\rho_{A,\ell}$ contains $\mathrm{Sp}_{2n}(A[\ell](\overline{K}))$, then the image of $\rho_{A,\ell}$ already coincides with $\mathrm{GSp}(A[\ell](\overline{K}))$.*

3 Compilation of tools

In this section, we discuss some tools from arithmetic geometry that we will use in the proof of our main theorem. We do so mainly for the convenience of the reader, but also to provide some complementary details.

3.1 Local constancy of p-adic families of Galois representations

In order to discuss Kisin's results on local constancy in p-adic families of Galois representations (cf. [14]), we need the language of étale fundamental groups. We refer to [12] Exp. V §4-7 for generalities on fundamental groups and in particular on étale fundamental groups for schemes. We will also need to use étale fundamental groups of rigid-analytic spaces, by which, following Kisin [14], we mean the *algebraic* étale fundamental groups defined in [9]. If U is a connected scheme or a connected rigid space and if $\bar{x}$ is a geometric point of U, we let $F_{U,\bar{x}}$ denote the associated fiber functor from the category of finite étale U-objects to the category of finite sets. By [12] Exp. V Cor. 5.7, any two such fiber functors are isomorphic. If $\bar{y}$ is another geometric point of U, then an isomorphism of fiber functors $F_{U,\bar{y}} \cong F_{U,\bar{x}}$ will also be called an *étale path* from $\bar{y}$ to $\bar{x}$ inside U. Since the étale fundamental group $\pi_1(U,\bar{x})$ of U at $\bar{x}$ is, by definition, the group of automorphisms of the functor $F_{U,\bar{x}}$, any étale path $F_{U,\bar{x}} \cong F_{U,\bar{y}}$ gives rise to an isomorphism $\pi_1(U,\bar{x}) \cong \pi_1(U,\bar{y})$, and the étale paths $\bar{x} \sim \bar{x}$ correspond to the inner automorphisms of $\pi_1(U,\bar{x})$.

Let K be a field that is complete with respect to a nontrivial nonarchimedean valuation; in the following, we will also write $\mathrm{Spec}\, K$ instead of $\mathrm{Sp}\, K$, by abuse of notation. Let U be a connected K-scheme or a connected rigid K-variety, let p denote the structural morphism from U to $\mathrm{Spec}\, K$, and let us assume that U admits K-rational points

$$x, y \,:\, \mathrm{Spec}\, K \to U \ .$$

We fix an embedding of K into an algebraic closure $\overline{K}$ of K, we let $\overline{z}$ denote the corresponding geometric point of $\mathrm{Spec}\, K$, and we let $\bar{x}, \bar{y}$ denote the resulting geometric points of U above x and y respectively; then $\bar{x}$ and $\bar{y}$ map to $\overline{z}$ via the structural morphism $U \to \mathrm{Spec}\, K$. The morphism p induces identifications of fiber functors

$$F_{\bar{z}} \;=\; F_{U,\bar{x}} \circ p^* \;=\; F_{U,\bar{y}} \circ p^* \ , \quad (1)$$

while x and y induce identifications

$$\begin{aligned} F_{U,\bar{x}} &= F_{\bar{z}} \circ x^* \text{ and} \\ F_{U,\bar{y}} &= F_{\bar{z}} \circ y^* ; \end{aligned} \qquad (2)$$

here p^*, x^* are y^* denote the respective pullback functors on categories of finite étale schemes. By (1), an étale path $\alpha : F_{U,\bar{y}} \cong F_{U,\bar{x}}$ induces an automorphism β of $F_{\bar{z}}$; by (2), β induces an automorphism γ of $F_{U,\bar{x}}$. After modifying α by γ, we see:

Lemma 3.1. *There exists an étale path $F_{U,\bar{y}} \cong F_{U,\bar{x}}$ which induces the identity on $F_{\bar{z}}$.*

An étale path $\phi : F_{U,\bar{y}} \to F_{U,\bar{x}}$ as in Lemma 3.1 above induces a commutative diagram

$$\begin{array}{ccccccccc} & & & & & \overset{y}{\curvearrowleft} & & & \\ 1 & \longrightarrow & \pi_{1,\mathrm{geom}}(U,\bar{y}) & \longrightarrow & \pi_1(U,\bar{y}) & & \longrightarrow & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & & \downarrow{\scriptstyle \overline{\varphi}} & & \\ 1 & \longrightarrow & \pi_{1,\mathrm{geom}}(U,\bar{x}) & \longrightarrow & \pi_1(U,\bar{x}) & & \longrightarrow & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & 1 \end{array} \overset{x}{\curvearrowleft} ,$$

where the vertical maps are isomorphisms, where the geometric étale fundamental groups on the left are defined so that the rows in the diagram are exact, where we have identified $\pi_1(\mathrm{Spec}\, K, \bar{z})$ with $\mathrm{Gal}(\overline{K}/K)$ and where $\bar{\varphi}$ is the identity on $\mathrm{Gal}(\overline{K}/K)$. We then have a commutative diagram

$$\begin{array}{ccc} F_{U,\bar{y}}(\cdot) & \xrightarrow[\sim]{\phi} & F_{U,\bar{x}}(\cdot) \\ \circlearrowleft & & \circlearrowleft \\ \pi_1(U,\bar{y}) & \xrightarrow[\sim]{\varphi} & \pi_1(U,\bar{x}) \\ {\scriptstyle y}\uparrow\downarrow & & {\scriptstyle x}\uparrow\downarrow \\ \mathrm{Gal}(\overline{K}/K) & = & \mathrm{Gal}(\overline{K}/K) \end{array} \qquad (3)$$

Let now A be a principally polarized abelian U-scheme, and let ℓ be a prime number; then $A[\ell]$ and μ_ℓ are finite étale U-schemes, and the symplectic structures on the geometric fibers of $A[\ell]$ are induced from morphisms of finite étale U-schemes

$$\begin{aligned} + &: A[\ell] \times A[\ell] \to A[\ell] \quad \text{and} \\ \langle \cdot, \cdot \rangle &: A[\ell] \times A[\ell] \to \mu_\ell . \end{aligned}$$

Since $\pi_1(U,\bar{x})$ is the automorphism group of the *functor* $F_{U,\bar{x}}$, it thus acts on $F_{U,\bar{x}}(A[\ell])$ via symplectic automorphisms, that is, the image of the natural map

$$\rho_{\bar{x}} : \pi_1(U,\bar{x}) \to \mathrm{Aut}(F_{U,\bar{x}}(A[\ell]))$$

lies in $\mathrm{GSp}(F_{U,\bar{x}}(A[\ell]))$, and the analogous statement holds for $\bar{y}$. Similarly, since ϕ is an isomorphism of fiber *functors*, the isomorphism $\phi(A[\ell]) : F_{U,\bar{y}}(A[\ell]) \xrightarrow{\sim} F_{U,\bar{x}}(A[\ell])$ respects

symplectic structures, so we obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{GSp}(F_{U,\bar{y}}(A[\ell])) & \xrightarrow[\sim]{\phi} & \mathrm{GSp}(F_{U,\bar{x}}(A[\ell])) \\ \uparrow & & \uparrow \\ \pi_1(U,\bar{y}) & \xrightarrow[\sim]{\varphi} & \pi_1(U,\bar{x}) \\ {\scriptstyle y}\uparrow\downarrow & & {\scriptstyle x}\uparrow\downarrow \\ \mathrm{Gal}(\overline{K}/K) & = & \mathrm{Gal}(\overline{K}/K)\ . \end{array} \tag{4}$$

Let now S be a connected K-scheme of finite type, let us assume that K has positive residue characteristic, and let x be a K-rational point of S. If X is any finite étale S-scheme, then by a main result of Kisin's article [14], there exists an admissible open neighborhood U of x in the rigid analytification S^{an} of S such that the action of $\pi_1(U,\bar{x})$ on the fiber $F_{U,\bar{x}}(X)$ factors through the section x. In other words, if

$$\rho_{\bar{x}} \,:\, \pi_1(U,\bar{x}) \to \mathrm{Aut}(F_{U,\bar{x}}(X))$$

is the natural homomorphism, if $\pi_{\bar{x}}$ is the natural projection from $\pi_1(U,\bar{x})$ onto $\mathrm{Gal}(\overline{K}/K)$ and if x is its given section, then $\rho_{\bar{x}} = \rho_{\bar{x}} \circ x \circ \pi_{\bar{x}}$. Let now A be an abelian scheme over S; we choose an admissible open neighborhood U of x in S^{an} such that U satisfies the conclusion of Kisin's theorem for both $A[\ell]$ and μ_ℓ; this is possible since intersections of admissible open subspaces of S^{an} are again admissible open in S^{an}. Then for any K-rational point y of U and any étale path $\phi : F_{\bar{y}} \xrightarrow{\sim} F_{\bar{x}}$ inside U satisfying the condition of Lemma 3.1, we obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{GSp}(F_{\bar{y}}(A[\ell])) & \xrightarrow{\sim} & \mathrm{GSp}(F_{\bar{x}}(A[\ell])) \\ {\scriptstyle y}\uparrow & & {\scriptstyle x}\uparrow \\ \mathrm{Gal}(\overline{K}/K) & = & \mathrm{Gal}(\overline{K}/K)\ . \end{array}$$

We conclude:

Theorem 3.2. *If K is a field that is complete with respect to a nontrivial nonarchimedean valuation of positive residue characteristic, if S is a connected K-scheme of finite type, if x is a K-rational point of S, if A is a principally polarized abelian S-scheme and if ℓ is any prime number, then there exists an admissible open neighborhood U of x in the rigid analytification S^{an} of S such that for all K-rational points y of U and for any choice of (symplectic) $\mathbb{F}_\ell$-bases of $A[\ell]_x(\overline{K})$, $A[\ell]_y(\overline{K})$ and $\mu_\ell(\overline{K})$, the natural representations*

$$\rho_x, \rho_y \,:\, G_K \to \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$$

coincide up to conjugation by an element of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$, where n denotes the dimension of A.

3.2 Existence of global points

We quote a special case of a theorem of Moret-Bailly, cf. [17] and [7] Theorem 3.1:

Theorem 3.3. *Let K be a number field, let X be a smooth geometrically connected K-variety, let K'/K be a finite field extension, let S be a finite set of (possibly infinite) places of K, and for each $\nu \in S$, let Ω_ν be a nonempty ν-adically open subset of $X(K_\nu)$. Then there exists a finite extension F/K that is linearly disjoint to K'/K, together with an F-rational point $x \in X(F)$ such that for each $\nu \in S$*

(*i*) *the place ν splits completely in F, and*

(*ii*) *for every place $\tilde{\nu}$ of F above ν, $x_{\tilde{\nu}} \in \Omega_\nu$ via the resulting natural identification*

$$X(F_{\tilde{\nu}}) \cong X(K_\nu) \, .$$

Remarks 3.4. Let us note:

(i) If X is as in Theorem 3.3 above and if $U \subseteq X_{K_\nu}^{\mathrm{an}}$ is an admissible open subset of the analytification of X_{K_ν}, then $U(K_\nu) \subseteq X(K_\nu)$ is ν-adically open.

(ii) Let $j \geq 3$ be an integer, and let K be a number field containing the j-th roots of unity; then the moduli space $\mathcal{A}_{n,1,j/K}$ of principally polarized n-dimensional abelian schemes with full symplectic level j structure above K is a smooth and geometrically connected K-scheme, cf. [10] Chap. IV Def. 6.1, Rem. 6.2 (c) and Cor. 5.10.

4 Existence of abelian varieties

4.1 Existence of ℓ-torsion approximations

We first apply the techniques of Sections 3.1 and 3.2 to the problem of finding abelian varieties A defined over finite extensions F of a given number field K such that, locally at the places of F lying above a finite number of finite places ν of K, the ℓ-torsion of A coincides with the ℓ-torsion of given abelian varieties that are defined over the local fields K_ν.

Definition 4.1. Let K be a number field, and let $n \geq 1$, $j \geq 1$ be integers. A local AV-datum (with level j-structure) of dimension n over K is a finite set S of finite places of K together with a family $(A_\nu \, ; \, \nu \in S)$, where A_ν is an n-dimensional principally polarized abelian variety over K_ν (with full symplectic level j structure). By abuse of notation, such a local AV-datum (with level j-structure) will be simply denoted by $(A_\nu \, ; \, \nu \in S)$.

Definition 4.2. Let K be a number field, and let $(A_\nu \, ; \, \nu \in S)$ be a local AV-datum of dimension n over K. An ℓ-torsion approximation of $(A_\nu \, ; \, \nu \in S)$ is a pair (F, A), where F/K is a finite field extension that is totally split in S and where A is a principally polarized abelian F-variety such that for each $\nu \in S$, for each place $\tilde{\nu}$ of F above ν and for any choice of symplectic $\mathbb{F}_\ell$-bases, the representations

$$\rho_{A_\nu,\ell} \text{ and } \rho_{A,\ell|_{D_{\tilde{\nu}}}} \, : \, G_{F_{\tilde{\nu}}} \to \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$$

are conjugate.

As we shall now see, the results of Kisin and Moret-Bailly show that ℓ-torsion approximations (F, A) of local AV-data with level j structure exist whenever $j \geq 3$ and $K \supset \mu_j$, even if one requires F/K to be linearly disjoint from a given finite extension field K'/K. Heuristically speaking, Kisin's results show that a local AV-datum gives rise, via its ℓ-torsion representations, to a family of congruence conditions on the moduli space, while Moret-Bailly's theorem tells us that these congruence conditions admit a global solution.

Theorem 4.3. *Let K be a number field, let $j \geq 3$ be an integer such that $\mu_j(\overline{K}) \subseteq K$, and let $(A_\nu\,;\,\nu \in S)$ be a local AV-datum with level j-structure over K. Then for each prime number ℓ and for each finite field extension K'/K, there exists an ℓ-torsion approximation (F, A) of $(A_\nu\,;\,\nu \in S)$ such that F/K is linearly disjoint to K'/K.*

Proof. Let n denote the dimension of $(A_\nu\,;\,\nu \in S)$, and let us write $\mathcal{A}$ to denote the moduli space $\mathcal{A}_{n,1,j/K}$ of n-dimensional principally polarized abelian schemes with full symplectic level j structure over K, cf. Remark 3.4 (ii) above. For each $\nu \in S$, let x_ν denote the K_ν-valued point of $\mathcal{A}$ corresponding to A_ν. By Kisin's theory (cf. Theorem 3.2 above), we may choose, for each $\nu \in S$, a ν-adically open neighborhood Ω_ν of x_ν in $\mathcal{A}(K_\nu)$ such that for any $y_\nu \in \Omega_\nu$, the representations $\rho_{x_\nu} : G_{K_\nu} \to \mathrm{GSp}(A_\nu[\ell](\overline{K}_\nu)) \simeq \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ and $\rho_{y_\nu} : G_{K_\nu} \to \mathrm{GSp}(B_\nu[\ell](\overline{K}_\nu)) \simeq \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ coincide up to conjugation with an element of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$, where B_ν denotes the abelian K_ν-variety that is given by y_ν. By Moret-Bailly's theorem (cf. Theorem 3.3 above), there exists a finite extension F/K linearly disjoint to K'/K with a point $y \in \mathcal{A}(F)$ such that each $\nu \in S$ splits completely in F and such that for each $\nu \in S$ and each place $\tilde{\nu}$ of F lying above ν, the localization $y_{\tilde{\nu}} \in \mathcal{A}(F_{\tilde{\nu}})$ of $y \in \mathcal{A}(F)$ lies in Ω_ν, where we use the natural isomorphism $\mathcal{A}(F_{\tilde{\nu}}) \cong \mathcal{A}(K_\nu)$ to regard Ω_ν as a subset of $\mathcal{A}(F_{\tilde{\nu}})$. The point y now defines a principally polarized abelian variety A over F such that for all $\nu \in S$ and all places $\tilde{\nu}$ of F above ν, $\rho_{A,\ell}|_{D_{\tilde{\nu}}}$ and $\rho_{A_\nu,\ell}$ coincide up to conjugation by an element of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. □

4.2 Local conditions enforcing big image

Definition 4.4. Let K be a number field, let A be a principally polarized abelian K-variety, and let ℓ be a prime number. We say that A has big image at ℓ if the natural homomorphism

$$\rho_{A,\ell} : G_K \to \mathrm{GSp}(A[\ell](\overline{K}))$$

is surjective.

Given an abelian variety A defined over a field K, we will denote by $K(A[\ell])$ the finite Galois extension of K defined by the kernel of $\rho_{A,\ell}$.

Lemma 4.5. *Let K be a number field, let A be a principally polarized abelian K-variety with big image at a prime number ℓ, let S be any finite set of finite places of K, and let $C \subseteq \mathrm{GSp}(A[\ell](\overline{K}))$ be a conjugacy class. Then there exists a finite place ν of K away from S such that $\rho_{A,\ell}$ is unramified at ν and such that $\rho_{A,\ell}(\mathrm{Frob}_\nu) \in C$. If moreover $j \geq 1$ is an integer such that $K(A[\ell])$ and $K(A[j])$ are linearly disjoint over K, there exists such a place ν with the additional property that $A \otimes_K K_\nu$ admits a full symplectic level j structure.*

Proof. Let $L = K(A[\ell])$, let K' denote the field $K(A[j])$ if we are given an integer $j \geq 1$ as in the statement, and let us set $K' = K$ otherwise. Then in both bases, L and K' are linearly disjoint over K. It suffices to find a positive density set of finite places ν of K such that L/K is unramified at ν, such that $\rho_{A,\ell}(\mathrm{Frob}_\nu) \in C$ and such that ν splits completely in K'. By [18] Lemma 13.5, it thus suffices to find a positive density set of finite places ν of K such that ν is unramified in LK' (hence in L and K'), such that $\rho_{A,\ell}(\mathrm{Frob}_\nu) \in C$ and such that Frob_ν restricts to the trivial automorphism of K'/K. By the Čebotarev density theorem (cf. [18] Thm. 13.4), it thus suffices to show that inside $\mathrm{Gal}(LK'/K)$, the $\rho_{A,\ell}$-preimage of C and $\mathrm{Gal}(LK'/K')$ have nonempty intersection. This, however, follows from the fact that the restriction of $\rho_{A,\ell}$ to $G_{K'}$ is surjective, which in turn follows from the fact that $\rho_{A,\ell}$ is surjective and from the fact that L and K' are K-linearly disjoint. □

Proposition 4.6. *Given a number field K and integers $n, j \geq 1$, there exist an integer $\ell_0 \geq 1$ such that for every prime $\ell \geq \ell_0$, there exists a finite field extension K''/K such that for every finite field extension K'/K that is linearly disjoint from K''/K, there exists a set S of two finite places of K' away from any given finite set of finite places of K' and a local AV-datum with level j structure $(J_\nu\,;\,\nu \in S)$ such that every ℓ-torsion approximation (F, A) of $(J_\nu\,;\,\nu \in S)$ with F being K'-linearly disjoint to $K'(\mu_\ell)$ has big image at ℓ.*

Proof. By the appendix of [13], there exists a hyperelliptic curve of genus n above K whose Jacobian J has trivial endomorphism ring over $\overline{K}$ and satisfies Hall's condition

(T) : There exists a finite extension L/K such that the Néron model of $J \otimes_K L$ over $\mathcal{O}_L$ has a semi-stable fiber with toric dimension one.

This property is preserved under finite extensions of K. By Theorem 1 of [13], there exists a natural number ℓ_0 such that for any prime number $\ell \geq \ell_0$, $J \otimes_K K(J[j])$ has big image at ℓ. Then J has big image at ℓ as well, and the fields $K(J[\ell])$ and $K(J[j])$ are K-linearly disjoint. After enlarging ℓ_0, we may in addition assume that $K/\mathbb{Q}$ is unramified at all primes $\ell \geq \ell_0$; then $[K(\mu_\ell) : K] = \ell - 1$ for all primes $\ell \geq \ell_0$, and hence ℓ_0 satisfies the conclusion of Lemma 2.4 for K. By Proposition 6.2 of the appendix to this paper, we may, after possibly further enlarging ℓ_0 (so that $\ell_0 \geq \max\{5, p : p|n\}$), assume that for every prime $\ell \geq \ell_0$, $\mathrm{GSp}(J[\ell](\overline{K}))$ contains an irreducible element $\mathfrak{s}_\ell$ of nonzero trace and a transvection $\mathfrak{t}_\ell$. Let us now fix a prime number $\ell \geq \ell_0$, let us set $K'' := K(J[\ell], J[j])$, and let K'/K be a finite field extension that is linearly disjoint from K''/K; then $J \otimes_K K'$ has big image at ℓ, and $[K'(\mu_\ell) : K'] = \ell - 1$. By Lemma 4.5, there exist finite places ν_s and ν_t of K' away from any given finite set of finite places of K' such that the image of $J_{\nu_s} := J \otimes_K K'_{\nu_s}$ at ℓ contains $\mathfrak{s}_\ell$, such that the image of $J_{\nu_t} := J \otimes_K K'_{\nu_t}$ at ℓ contains $\mathfrak{t}_\ell$ and such that both J_{ν_s} and J_{ν_t} admit a full symplectic level j structure. Indeed, $K'(J[\ell])$ and $K'(J[j])$ are K'-linearly disjoint because $K(J[\ell])$ is K-linearly disjoint to $K(J[j])$ and because K' is K-linearly disjoint to $K'' = K(J[\ell], J[j])$. Let us set $S := \{\nu_s, \nu_r\}$, and let $(J_\nu\,;\,\nu \in S)$ be the resulting local AV-datum with level j structure. Let now (F, A) be an ℓ-torsion approximation of $(J_\nu\,;\,\nu \in S)$ such that F and $K'(\mu_\ell)$ are K'-linearly disjoint. Then $[F(\mu_\ell) : F] = \ell - 1$, so F satisfies the conclusion of Lemma 2.4, and the image of A at ℓ contains the symplectic group by Theorem 2.1. It follows that A has big image at ℓ, as desired. □

Let us note that we can always take $K' = K$ in the statement of Proposition 4.6. However, it will prove useful later to have the full strength of Proposition 4.6 at one's disposal, i.e. to be

able to obtain a local AV-datum as in the conclusion of Proposition 4.6 over a rather general finite field extension K' of K.

Remark 4.7. The constant ℓ_0 from Proposition 4.6 is explicit, and it depends only on K, n and j. Indeed, given K and n, we can fix a hyperelliptic curve C of genus n defined over K with trivial endomorphism ring and satisfying Hall's condition (cf. Appendix to [13]). Denote by J_C its Jacobian. Fix $j \geq 1$; there are explicit formulas for the field $K(J_C[j])$ (cf. [8]). Let p_0 be the biggest prime number that ramifies in $K(J_C[j])$. Theorem 1 of [13] provides an explicit constant ℓ_0' depending only on J_C and $K(J_C[j])$ such that for all $\ell \geq \ell_0'$, $\rho_{J,\ell} : G_{K(J_C[j])} \to \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ is surjective. In the proof of Proposition 4.6 above, we have taken

$$\ell_0 = \max\{\ell_0', p_0, 5, p : p|n\} ;$$

hence our constant ℓ_0 is effective.

4.3 Local conditions enforcing tameness

Proposition 4.8. *Let K be a number field, let $n, j \geq 1$ be integers, let S, S' be finite disjoint sets of finite places of K, and let ℓ be a prime avoiding both j and S'. There exists a finite extension K'/K together with an n-dimensional local AV-datum with level j structure $(A_\nu ; \nu \in T)$ over K', where T denotes the set of places of K' over S, such that K'/K is unramified in the places above ℓ, such that K'/K is totally ramified over S' and such that the ℓ-torsion representations of the A_ν are tamely ramified.*

Proof. We may assume that S contains all places above ℓ. For every place $\nu \in S$, let us choose an elliptic curve E_ν over $\mathbb{Q}$ such that E_ν has good reduction and such that E_ν has good supersingular reduction whenever ν divides ℓ; for the existence of these elliptic curves see for instance [3] Cor. 3.6 and Prop. 3.7. Let us then set $K_\nu' := K_\nu(E_\nu[j])$. If ν is a place above ℓ, the Néron-Ogg-Shafarevich criterion implies that the extension K_ν'/K_ν is unramified (recall that $\ell \nmid j$).

After possibly enlarging the K_ν' by means of unramified extensions, we may assume that the degrees $[K_\nu' : K_\nu]$ all coincide; let r denote this common degree. For each $\nu \in S'$, let K_ν'/K_ν be a totally ramified extension of degree r, obtained for instance by extracting an r-th root of a uniformizer of K_ν. There exists a finite extension K'/K of degree r such that the induced local extensions at $S \cup S'$ coincide with the K_ν'/K_ν: indeed, for each $\nu \in S \cup S'$, let α_ν be a primitive element for K_ν'/K_ν, and let $f_\nu \in K_\nu[X]$ be its minimal polynomial. By the weak approximation theorem (cf. [6] Chap. VI §7 No. 3 Thm. 2), there exists a monic polynomial $f \in K[X]$ of degree r which approximates the f_ν simultaneously, up to a precision such that Krasner's Lemma (cf. [5] 3.4.2 Prop. 3 and Cor. 4) applies; we then set $K' = K[x]/(f)$. By construction, K'/K has the desired ramification behavior. For each $\nu \in S$, let us consider the abelian variety $A_\nu = E_\nu^n$ over K_ν'. Then A_ν admits a full symplectic level j structure, and furthermore, the ℓ-torsion representation of A_ν is tamely ramified. For $\nu|\ell$, this follows from [19] Prop. 13, and for $\nu \in S$ not dividing ℓ, the Néron-Ogg-Shafarevich criterion (cf. [20] Theorem 1) even guarantees that $\rho_{A_\nu,\ell}$ is unramified. □

Remark 4.9. In the Situation of Proposition 4.8, if S is the set of places of K lying above the set of rational primes dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ and if (F, A) is an ℓ-torsion approximation of $(A_\nu\,;\,\nu \in T)$, then the ℓ-torsion representation of A is everywhere tamely ramified.

4.4 Existence of ℓ-torsion approximations with big image

Proposition 4.10. *Let K be a number field, and let $n \geq 1$, $j \geq 3$ be integers such that $\mu_j(\overline{K}) \subseteq K$. Then there exists a constant ℓ_0 such that for every prime number $\ell \geq \ell_0$, there exists a finite extension K''/K such that for every finite extension K'/K that is linearly disjoint to K''/K, every n-dimensional local AV-datum with level j structure over K' admits an ℓ-torsion approximation with big image at ℓ.*

Proof. Let us choose ℓ_0 as in Proposition 4.6, let $\ell \geq \ell_0$ be a prime number, let K''/K be as in Proposition 4.6, let K'/K be a finite extension that is linearly disjoint to K''/K, and let $(A_\nu\,;\,\nu \in S)$ be an n-dimensional local AV-datum with level j structure over K'. By Proposition 4.6, there exists an n-dimensional local AV-datum with level j structure $(J_\nu\,;\,\nu \in S')$ over K' such that S' is disjoint to S and such that the conclusion of Proposition 4.6 holds. For $\nu \in S'$, let us write $A_\nu := J_\nu$. By Theorem 4.3, there exists an ℓ-torsion approximation (F, A) of $(A_\nu\,;\,\nu \in S \cup S')$ such that F is linearly disjoint to $K'(\mu_\ell)$ over K'. Then (F, A) is an ℓ-torsion approximation of both $(A_\nu\,;\,\nu \in S)$ and $(J_\nu\,;\,\nu \in S')$; by Proposition 4.6, it follows that A has big image at ℓ. □

Let us note that in the statement of Proposition 4.10, we can always choose $K' = K$.

5 Proof of the main result

We can now give the proof of Theorem 1.1. Let us restate it:

Theorem 5.1. *Given a number field K and an integer $n \geq 1$, there exists an integer ℓ_0 such that for all prime numbers $\ell \geq \ell_0$, there exist a finite extension F of K, unramified in all places above ℓ, and an n-dimensional abelian variety A defined over F such that the ℓ-torsion representation of A is surjective and everywhere tamely ramified.*

Proof. Let us fix any $j \geq 3$. If K'/K is a finite extension and if ℓ_0' is a constant such that the statement of the theorem holds for K' and ℓ_0', then the theorem holds for K and any constant $\ell_0 \geq \ell_0'$ such that K'/K is unramified in all places above the rational primes $\ell \geq \ell_0$. We may thus replace K by a finite extension and hereby assume that $\mu_j(\overline{K}) \subseteq K$. Let ℓ_0 be the constant given by Proposition 4.10. After possibly enlarging ℓ_0, we may assume that $\ell_0 > j$; then j is coprime to any prime number $\ell \geq \ell_0$. Let us fix a prime number $\ell \geq \ell_0$, let K''/K be the finite extension given by Proposition 4.10, let S denote the set of places of K dividing the order of $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$; then S contains all places above ℓ. Let moreover S' be the set consisting of a single finite place μ of K away from S such that K''/K is unramified at μ. Let K'/K and $(A_\nu\,;\,\nu \in T)$ be the associated data given by Proposition 4.8; then K'/K

is totally ramified at μ, while K''/K is unramified in μ, and it follows from [11] Lemma 2.5.8 that K' and K'' are linearly disjoint over K. By Proposition 4.10, there exists an ℓ-torsion approximation (F, A) of $(A_\nu\,;\,\nu \in T)$ with big image at ℓ. Now F/K' is totally split over T, K'/K is unramified in the places above ℓ, and T contains all places of K' above ℓ. The pair (F, A) thus has the desired properties. □

Our methods can be used to prove the following strengthening of Theorem 1.1:

Theorem 5.2. *Let K be a number field, let $n \geq 1$ be an integer, and let ℓ_0 be the constant given by Theorem 5.1 and its proof, for some $j \geq 3$. Then for all primes $\ell \geq \ell_0$, the pairs (F, A) satisfying the conclusion of Theorem 1.1 lie Zariski-dense in the moduli-space $\mathcal{A} = \mathcal{A}_{n,1,j/K}$ (cf. Remark 3.4 (ii)). In particular, there exist infinitely many pairwise geometrically non-isomorphic such pairs.*

Proof. Indeed, let us assume that all these points lie on a proper closed subvariety $V \subsetneq \mathcal{A}$, and let U denote the complement of V in $\mathcal{A}$. We argue exactly as above, except that in the proof of Theorem 4.3, we apply Theorem 3.3 to U and to the intersections

$$\Omega'_\nu \,:=\, \Omega_\nu \cap U(K_\nu)\,;$$

Theorem 3.3 applies to this input data because U is smooth and geometrically irreducible and because the sets Ω'_ν are again open and non-empty, where non-emptiness follows by dimension reasons from the openness of the Ω_ν. The pair (F, A) that is produced by the proof of Theorem 5.1 then defines an F-valued point of U, contrary to our assumption. □

Remark 5.3. One may wonder whether for a fixed finite extension F/K that is unramified in the places above ℓ, the pairs (F, A) satisfying the conditions of Theorem 5.1 lie dense in the moduli, or one may ask the weaker question whether there exist infinitely many pairwise non-isomorphic such pairs. At present we do not know how to obtain such a result.

6 Appendix

Definition 6.1. Let q be a power of a prime p, and let $\mathbb{F}_q$ be the field with q elements. Let $f \in \mathbb{F}_q[x]$ be a monic polynomial.

(i) Write $f(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0$. We say that a_{r-1} is the *trace* of $f(x)$.

(ii) Assume the degree of f is $2n$ for some $n \in \mathbb{N}$. We say that f is *symplectic* if it satisfies that $a_i = a_{2n-i}$ for all $i = 1, \ldots, n$ and $a_0 = 1$, that is, if $f(x)$ has the shape

$$x^{2n} + a_1x^{2n-1} + \cdots + a_{n-1}x^{n+1} + a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + 1.$$

It is easily seen that $f(x)$ is symplectic if and only if it satisfies the relation

$$x^{2n} f\left(\frac{1}{x}\right) = f(x)$$

in the field $\mathbb{F}_q(x)$.

In this appendix, we give a proof of the following result:

Proposition 6.2. *For any positive integer $n \geq 1$, for all prime numbers $p \nmid n$ and for all $r \in \mathbb{N}$ such that $p^r \geq 5$, the ring $\mathbb{F}_{p^r}[X]$ contains an irreducible symplectic polynomial of nonzero trace and of degree $2n$.*

The proof will follow from a series of elementary lemmas.

Lemma 6.3. *Let q be a prime power, let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$ be a monic irreducible polynomial, and let $\alpha \in \overline{\mathbb{F}}_q$ be a root. Let β be a root of $x^2 - \alpha x + 1$, and let us assume that $\beta \notin \mathbb{F}_q(\alpha)$. Then the minimal polynomial of β over $\mathbb{F}_q$ is symplectic, and*

$$\mathrm{tr}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(\alpha) = \mathrm{tr}_{\mathbb{F}_q(\beta)/\mathbb{F}_q}(\beta).$$

Proof. Let us note that $\alpha = \beta + \frac{1}{\beta}$, and let us consider the polynomial $g(x) = x^n f\left(x + \frac{1}{x}\right) \in \mathbb{F}_q[x]$; then $g(x)$ is a symplectic polynomial satisfying $g(\beta) = 0$. Since $\mathbb{F}_q(\beta)$ has degree $2n$ over $\mathbb{F}_q$ and since $g(x)$ is a monic polynomial of degree $2n$, $g(x)$ must be the minimal polynomial of β over $\mathbb{F}_q$. Therefore $\mathrm{tr}_{\mathbb{F}_q(\beta)/\mathbb{F}_q}(\beta)$ is equal to the coefficient of x^{2n-1} in $g(x)$, that is to say, a_{n-1}, which is precisely $\mathrm{tr}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(\alpha)$. □

To prove Proposition 6.2, it now suffices to show that for p not dividing n and for $q = p^r \geq 5$, we can find an $\alpha \in \overline{\mathbb{F}}_q$ with $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ of degree n and nonzero trace such that the polynomial $x^2 - \alpha x + 1$ is irreducible.

Lemma 6.4. *If p is a prime number, if q is a power of p and if $n \geq 1$ such that $p \nmid n$, then the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n and nonzero trace is equal to*

$$\frac{q-1}{qn} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Proof. The number of monic irreducible polynomials of degree n is $\frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$ (cf. Theorem 3.25 of [16]). On the other hand, we can define an equivalence relation on the set of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ by declaring that $f \equiv g$ if and only if there exists an $a \in \mathbb{F}_q$ with $f(x) = g(x - a)$. Each equivalence class consists of precisely q elements, and the traces of the representatives of any given class are all distinct. Hence for each $a \in \mathbb{F}_q$, the cardinality of the set of monic irreducible polynomials with trace equal to a is $\frac{1}{qn}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$. □

Lemma 6.5. *Let q be a prime power, and let n be a positive integer; then the number of elements $\alpha \in \mathbb{F}_{q^n}$ such that $x^2 - \alpha x + 1$ is reducible over $\mathbb{F}_{q^n}$ equals*

$$\begin{cases} \frac{q^n+1}{2} & \text{if } q \text{ is odd and} \\ \frac{q^n}{2} & \text{if } q \text{ is even.} \end{cases}$$

Proof. Let α be any element of $\mathbb{F}_{q^n}$; then the polynomial $x^2 - \alpha x + 1$ is reducible over $\mathbb{F}_{q^n}$ if and only if $\alpha = \beta + \frac{1}{\beta}$ for some $\beta \in \mathbb{F}_{q^n}$. Let us consider the map

$$\phi : \mathbb{F}_{q^n}^{\times} \to \mathbb{F}_{q^n} \quad ; \quad \beta \mapsto \beta + \frac{1}{\beta} ;$$

we have to compute the cardinality of its image. To do so, we compute the cardinalities of the fibers of ϕ: let us consider an element $\alpha \in \mathbb{F}_{q^n}$ that lies in the image of ϕ, i.e. for which the quadratic equation

$$f_\alpha(x) \;=\; x^2 - \alpha x + 1 \;\in \mathbb{F}_{q^n}[x]$$

has a root β in $\mathbb{F}_{q^n}$; then $1/\beta$ is also a root of the above equation. Let us note that $\beta = 1/\beta$ if and only if $\beta = \pm 1$. Hence, if $\beta \neq \pm 1$, the cardinality of $\phi^{-1}(\alpha)$ is 2, since $f_\alpha(x)$ can have at most two different roots. On the other hand, if $\beta = \pm 1$, then the cardinality of $\phi^{-1}(\alpha)$ is 1, because β is then a multiple root of $f_\alpha(x)$: indeed, then

$$f'_\alpha(x) \;=\; 2x - \alpha \;=\; 2x - (\beta + \frac{1}{\beta}) = 2x - 2\beta$$

vanishes in β. Let us moreover note that if q is odd, then $\phi(1) = 2$ is different from $\phi(-1) = -2$. Since $\mathbb{F}_{q^n}^\times$ is the disjoint union of the fibers of ϕ, we conclude that for q odd,

$$q^n - 1 \;=\; 2 \cdot (|\mathrm{im}(\phi)| - 2) + 1 + 1 \;,$$

whereas for q even,

$$q^n - 1 \;=\; 2 \cdot (|\mathrm{im}(\phi)| - 1) + 1 \;;$$

the claim now follows by a straightforward computation. □

From Lemmas 6.4 and 6.5 we obtain the following result.

Lemma 6.6. *Let us assume that $p \nmid n$; then the number of $\alpha \in \overline{\mathbb{F}}_q$ with $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ of degree n, nonzero trace and such that the polynomial $x^2 - \alpha x + 1$ is irreducible over $\mathbb{F}_{q^n}$ is greater than or equal to*

$$\frac{q-1}{q} \sum_{d|n} \mu(d) q^{\frac{n}{d}} - \frac{q^n + 1}{2}$$

□

Proof of Proposition 6.2. Let us now assume that $q \geq 5$ and that $p \nmid n$. Combining Lemmas 6.3 and 6.6, we see that it suffices to prove that the number

$$M := \frac{q-1}{q} \sum_{d|n} \mu(d) q^{\frac{n}{d}} - \frac{q^n + 1}{2}$$

is positive. We distinguish two cases. First, if $n = 1$, then

$$M = \frac{q-1}{q} q - \frac{q+1}{2} = \frac{1}{2} q - \frac{3}{2} > 0$$

as desired. On the other hand, if $n > 1$, then

$$\begin{aligned} M &= \frac{q-1}{q}\sum_{d|n}\mu(d)q^{\frac{n}{d}} - \frac{q^n+1}{2} \\ &= \frac{q-1}{q}(q^n + \sum_{\substack{d|n \\ d\neq 1}}\mu(d)q^{\frac{n}{d}}) - \frac{q^n+1}{2} \\ &= \frac{1}{2}(q^n-1) - q^{n-1} + \frac{q-1}{q}\sum_{\substack{d|n \\ d\neq 1}}\mu(d)q^{\frac{n}{d}} \\ &\geq \frac{1}{2}(q^n-1) - q^{n-1} - \frac{q^n-1}{q-1} \\ &\geq \frac{1}{4}(q^n-1) - q^{n-1}\,, \\ &> 0 \end{aligned}$$

where for the third last inequality we used the inequalities $\mu(d) \geq -1$ and $(q-1)/q \leq 1$ as well as the geometric series. □

References

[1] Sara Arias-de-Reyna. Formal groups, supersingular abelian varieties and tame ramification. *J. Algebra*, 334:84–100, 2011.

[2] Sara Arias-de-Reyna, Luis Dieulefait, and Gabor Wiese. Compatible systems of symplectic Galois representations and the inverse Galois problem II. Transvections and huge image. *Preprint*, 2012.

[3] Sara Arias-de-Reyna and Núria Vila. Tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ over $\mathbb{Q}$. *J. Number Theory*, 129(5):1056–1065, 2009.

[4] Sara Arias-de-Reyna and Núria Vila. Tame Galois realizations of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ over $\mathbb{Q}$. *Int. Math. Res. Not. IMRN*, (9):2028–2046, 2011.

[5] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1990.

[6] Nicolas Bourbaki. *Commutative Algebra*. Elements of Mathematics. Springer-Verlag, 1989.

[7] Frank Calegari. Even Galois representations and the Fontaine–Mazur conjecture. II. *J. Amer. Math. Soc.*, 25(2):533–554, 2012.

[8] David G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *J. Reine Angew. Math.*, 447:91–145, 1994.

[9] A. J. de Jong. Étale fundamental groups of non-Archimedean analytic spaces. *Compositio Math.*, 97(1-2):89–118, 1995. Special issue in honour of Frans Oort.

[10] Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties*, volume 22 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1990.

[11] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.* Springer-Verlag, Berlin, third edition, 2008.

[12] A. Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris), 3, Lecture Notes in Math., 224, Springer, Berlin. Société Mathématique de France, 1960-61.

[13] Chris Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[14] Mark Kisin. Local constancy in p-adic families of Galois representations. *Math. Z.*, 230(3):569–593, 1999.

[15] Shang Zhi Li and Jian Guo Zha. On certain classes of maximal subgroups in $\mathrm{PSp}(2n, F)$. *Sci. Sinica Ser. A*, 25(12):1250–1257, 1982.

[16] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1986.

[17] Laurent Moret-Bailly. Groupes de Picard et problèmes de Skolem. II. *Annales scientifiques de l'É.N.S.*, 22(2):181–194, 1989.

[18] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[19] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[20] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88(3):492–517, 1968.